Survey Paper on CP-ABE cloud computing

Poornima G. Pawar, Prof. V. D. Thombre

Department of Computer Engineering, Savitribai Phule,Pune University SKN Institute of Technology & Science, Lonavala, Pune Maharashtra India

Abstract— *In attribute based encryption (ABE) scheme, attributes plays a very important role. Attribute –based encryption provides privacy protection for the users by a set of attributes. Now a days as cloud is most widely used in mostly all fields so there is need of keeping data more secure and confidential which is outsourced on the cloud. Security of the data in cloud database server is the key area of concern in the acceptance of cloud. It is required very high degree of privacy and authentication. In existing system used hierarchical authorization structure to reduce the burden and risk of a single authority .this paper proposes a hierarchical attribute based encryption which directly provides attribute value by user as well as data stored in different types of media*.

Keywords—Access control, attribute based encryption, multi-authority.

I. INTRODUCTION

in cloud computing, users store their data fields in cloud server, therefore it is very important[4] to prevent unauthorized access to these resources. cloud computing can provide several computing compatibilities, reduce cost and capital expenditure and change according to usage. The most suitable variant for fine-grained access control in the cloud cipher text policy CP-ABE.

Attribute based encryption is a version of public key encryption that allows users to encrypt and decrypt messages based on user attributes. Standard encryption is insufficient when numbers of users wants to share data between many users [7]; since the data need to be encrypted using every users public key. In many situations when a user encrypts sensitive data, it is imperative that she establish a specific access control policy on who can decrypt this data.

The scheme can be used to ensure fine-grain access control by the set of attributes [11] owned by the user. Attribute based encryption can be classified into two types:

1) Key policy ABE(KP-ABE)
2) Cipher Policy ABE (CP-ABE)

1) **Key Policy ABE:** The access Policies are associated with user's private key is generated based on the attribute values owned by the user.
2) **Cipher Policy ABE:** Access Policies are assigned with the cipher text .It is more flexible compared to KP-ABE.CP-ABE was first introduced by Amit Sahai and Brent Waters.

II. LITERATURE SURVEY

- **Title: attribute based access control for Multi Authority System in Cloud Storage**

Author: Kan Yang, Xiaohua Jia.

In this paper, a new access control framework for multi authority systems in cloud storage and propose an efficient and secure multi authority access control scheme. In designed an efficient multi authority CP-ABE scheme that does not require a global authority and can su support LSSS access structure. We proved that our multi-authority CP-ABE scheme provably secure in the random oracle model. We also proposed a new technique to solve the attribute revocation problem in multi authority CP-ABE scheme. We will remove the random oracle and extend our work to be provably secure in the standard model.

- **Title: Key-Policy attribute based encryption to secure data stored in cloud**

Author: C. Vinoth, G.R. Anantha Raman

In this paper the key policy attribute based encryption scheme, which provides more secure and fine-grained data access control in the system. It will be efficient and scalable to securely manage user data in the system. For key distribution the KDC is used. It is also helpful to secure data from the unauthorized user and auditors. The challenging problem is the construction of KP-ABE scheme with constant cipher text size and constant cipher text size and private key size.

- **Title: Attribute based access control**

Author: Prof. N.B. Kadu, Gholap Nilesh,Saraf Shashir, Garodi Pravin, Bora Anand

Attribute based access control provide data confidentiality. This system solves the drawbacks of role based access control by replacing attributes instead of roles.

We use constant size cipher text instead of depending linearly on numbers of attributes which helps to improve efficiency and performance. Our scheme maintains the size of cipher text and the computation of encryption and decryption at constant value.

- **Title: System Based access control for multi authority system with constant size cipher text in cloud computing.**

Author: Chen Yanil, Sng Linglish, Yang Geng

In this paper we presents a CP-ABE access control for multi authority system with constant size cipher text in cloud computing. Both the length of cipher text and the number of pairing operations in decryption are constant and independent of the number of attributes involved in the access structure, which reduce the communication and computing cost of the system. This scheme only supports a restricted access control structure, which is AND gates on multiple attributes.

- **Title: Attribute based access control for multi authority system with constant size cipher text in cloud computing**

Author: CHEN Yanil, SONG Lining, YANG Geng

In this paper we presents a CP-ABE access control for multi-authority systems with constant size cipher text in cloud computing. Both the length of cipher text and the number of pairing operations in decryption are constant and independent of the number of attributes involved in the access stricter, which reduce the communication and computing cost of multi authorities solve the escrow problem in the single authority system.

Title : Attribute based access control with constant size cipher text in cloud computing

Author: Wei Teng, Geng Yang, Yang Xiang, Ting Zhang, Dongyang Wang

Scheme sharing of data plays an important role in cloud computing. Attribute based access control can realized data confidentiality in the untrusted environment of server end, fine grained access control and large scale dynamic authorization which are difficult problems to solve the traditional access control. This paper proposes a structure of hierarchical attribute authority. This paper proposed a structure of hierarchical attribute authority based on cloud computing which reduces the burden and disperses the risk of the single authority. The propose scheme adopts CP-ABE with constant size cipher text that solves the problem of the cipher text size depending linearly on the number of attribute.

III. COMPARISON TABLE

Sr	Title	Author	Method Used	Drawbacks
1	attribute based access control for Multi Authority System in Cloud Storage	Kan Yang, Xiaohua Jia.	Global UID	Random selection attributes not supported to oracle
2	Key-Policy attribute based encryption to secure data stored in cloud	C. Vinoth, G.R. Anantha Raman	Proxy reencryption protocol used	It required TPA permission code
3	Attribute based access control	Prof. N.B. Kadu, Gholap Nilesh,Saraf Shashir, Sarodi Pravin,Bora Anand	Level Domain Authority	Can not transfer secure transfer file such as pdf,img,mp3,video
4	Attribute based access control for multi authority system with constant size cipher text	Chen Yanil, Sng Linglish, Yang Geng	q-BDHE	It only support restricted access structure
5	Attribute based access control	Wei Teng, Geng Yang,	Hierarchical metho	It required more secure parameters..

	with constant size cipher text in cloud computing	Yang Xiang, Ting Zhang, Dongyang Wang	d	

IV. CONCLUSION

In this paper we have studied many different techniques for how secure data in cloud computing. Existing methods having many drawbacks and limitations for attribute size for future work .we can use better algorithm to reduce burden of server and give fast throughput to the user.

ACKNOWLEDGMENT

We would like to thanks to our guide & respected teachers for their constant support and motivation for us. Our sincere thanks to SKN Sinhgad Institute of Technology and Science to develop our skill and capabilities.

REFERENCES

[1] Attribute based access control with constant size cipher text in cloud computing.
[2] Data management with attribute based encryption method for sensitive users in cloud computing. Vidyasagar Tella,L.V Ramesh.IJETR ISSN:2321-0869,vol-2,issue-9,September 2014
[3] Attribute based encryption Optimal for cloud computing(Mate Harvath) jan-5-2015
[4] Attribute based access control (Prof. N.B. Kadu ,Gholap Nilesh, Saraf Shashir, Garodi Pravin ,Bora Anand. IJARIIE-ISSN(0)-2395-4396vol-2,issue-2 2016
[5] Cipher Policy Hierarchical Attribute based encryption with short cipher text : Efficiently sharing data among large organizations.Hua Deng, Quanhong Wu,
[6] A Literature Survey on key aggregation system for secure sharing of cloud data. Arun Kumar S., S. Dhansekar IJARECE ,vlo-3, issue-(12 ,December 2014)
[7] An Efficient Presentation of Attribute Based Encryption Design in cloud data. ISSN:2277 128X, vol-5,issue-(2 Feb 2015)
[8] A survey on Attribute based encryption Scheme of Access control in cloud environment .IJNS, vol-15, no-4,pp.231-240,(July 2013)
[9] Attribute Based Access Control for Multi Authority System in cloud storage.32nd IEEE International conference on Distributed computing systems (2012)
[10] Attribute Based Access Control for multi Authority System with Constant size Ciphertext in cloud computing. China communucations(Feb 2016)
[11] Constant Size Ciphertext Attribute Based Encryption with Lively membership .Saranya P. P. Alphonsa Kurioakose(11 November 2015)
[12] Attribute Based Encryption schemes with Constant size Cipher texts(2010)
[13] Key-Policy attribute Based Encryption to Secure data stored in cloud IJATES vol-2,issue no-1,(September 2014)
[14] Enhancement of Cloud Computing Security with secure data storage using AES.IJIRST , vol-2, issue-09,February 2016.
[15] Cryptographic protocols for secure cloud computing.IJSIA, vol-10,no-2,pp:301-310(2016)